GLOBAL PERSPECTIVE ON DATA PROTECTION

Françoise Gilbert

IT Law Group

Palo Alto, CA 94301

fgilbert@itlawgroup.com

www.itlawgroup.com

TODAY'S BUSINESS IS GLOBAL BUSINESS

Companies

- Conduct business abroad through foreign offices, divisions, subsidiaries
- Have personnel working on several continents
- Outsource company functions to a foreign company: call center, hot line, support services
- Sell goods or services abroad, directly or through agents and reps
- Use directories that contain employee data or customer contact information worldwide
- Collect users information from company's website
- Enter into joint venture or strategic alliance with, or acquire foreign company

PRIVACY: USA V. THE WORLD

United States Privacy Laws:

- Sectoral approach: no federal or state legislation of general application
- Federal laws: financial, healthcare, children, video, electronic communications, etc.
- State laws: birth and death certificates access, driver's license, medical information, social security numbers, credit card numbers, etc.

THE REST OF THE WORLD

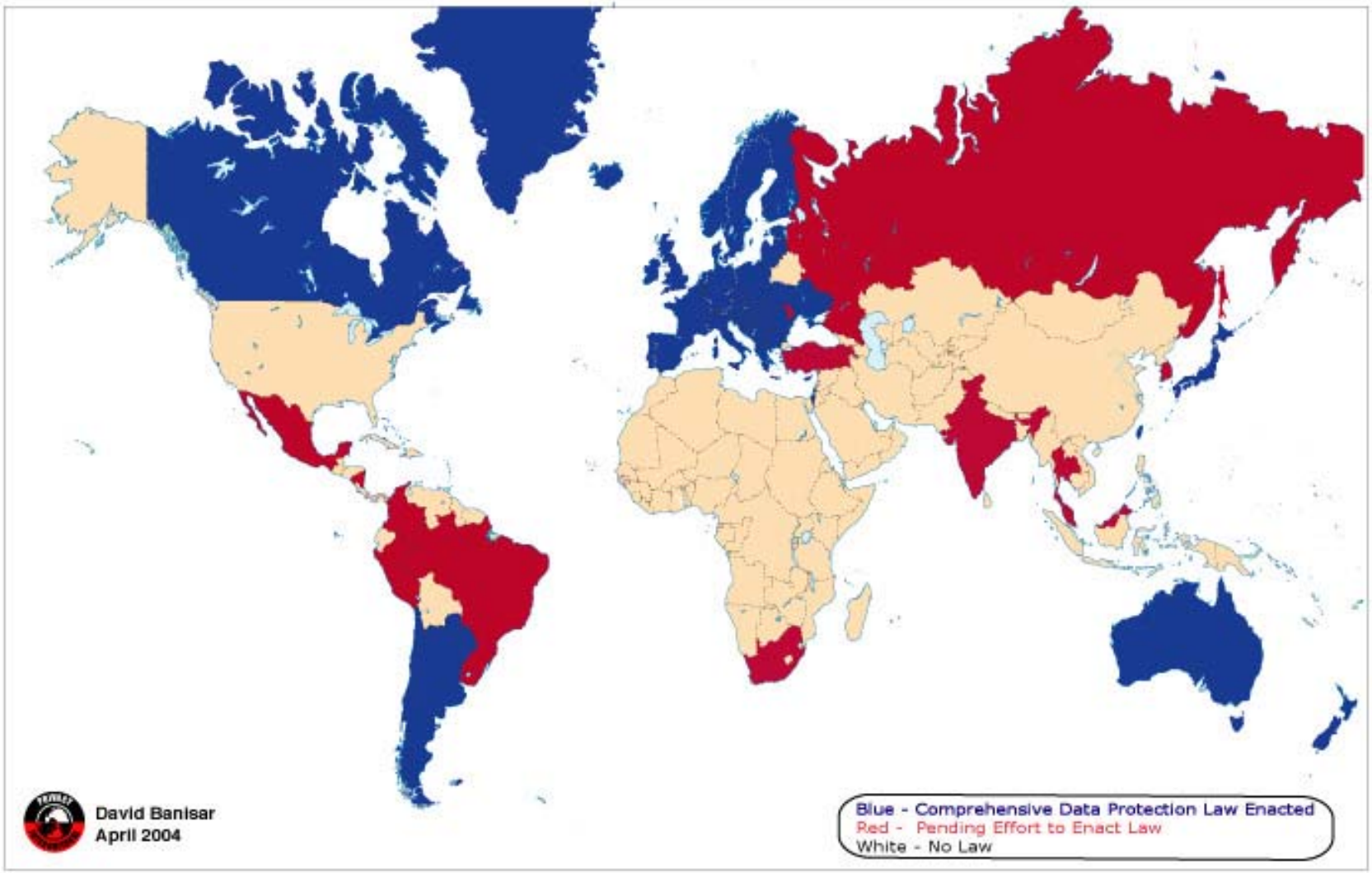
Foreign Privacy and/or Data Protection Laws:

- Laws of general application: one privacy law covers all aspects of privacy, and all types of data
- Generally follow the OECD Model
- Key element of concern for US companies: many foreign countries prohibit transfer of personal data to a country that does not have adequate privacy or data protection laws

HISTORY OF PRIVACY

- 1970 Germany: first data protection law in the Land of Hessen
- 1973 Sweden: Data Act, first comprehensive national data protection law
- 1974 US: Privacy Act (government)
- 1977 Germany: Federal Data Protection Law
- 1978 France: Data Protection Act
- 1978 Denmark: Privacy Registers Act and Public Registers Act
- 1978 US: Right to Financial Privacy Act (banks)
- 1978 Norway: Personal Data Registers Act
- 1979 Luxembourg: Act Concerning the Use of Nominal Data in Computer Processing
- 1984 United Kingdom: Data Protection Act

Data Protection Laws Around the World



EXAMPLES OF COUNTRIES WITH DATA PROTECTION LAWS

- 25 EU Members
- Argentina
- Australia
- Brazil
- Bulgaria
- Canada
- Chile
- Dominican Republic
- Hong Kong
- Iceland
- Israel
- New Zealand
- Norway
- Paraguay
- Uruguay
- Russia
- Switzerland
- Tunisia

LIMITED OR NO DATA PROTECTION

- Most of Asia except Russia
- China
- India
- Malaysia
- Philippines
- Singapore
- Central America
- Mexico
- Middle East except Israel
- Most of Africa

OECD LEADERSHIP

OECD - Organization for Economic Cooperation and Development

- First intergovernmental organization to issue guidelines on international policy for the protection of privacy in computerized data processing.
- 1980: *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* in support of the three principles that bind OECD member countries: pluralistic democracy, respect for human rights and open market economies
- 1985: *Declaration on Transborder Data Flows*
- *1998: Ministerial Declaration on the Protection of Privacy on Global Networks*

OECD PRIVACY GUIDELINES

- Guidelines represent international consensus on general guidance concerning the collection and management of personal information
- The principles contained in the OECD Privacy Guidelines are reflected in legislation and practices for the protection of privacy in many countries worldwide
- The principles set forth in the OECD Privacy Guidelines encompass:
  - all media used for the computerized processing of data on individuals (from local computers to networks with complex national and international ramifications)
  - all types of personal data processing (from personnel administration to the compilation of consumer profiles)
  - all categories of data (from traffic data to content data, from the most mundane to the most sensitive).

OECD PRIVACY GUIDELINES(2)

- Collection limitation
- Data quality
- Purpose specification
- Use limitation
- Security safeguards
- Openness
- Individual rights
- Accountability
- Free flow and legitimate restrictions

DATA PROTECTION IN THE EU

- **Directive 95/46/EC** (October 24, 1995) on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data
  - Key element: no transfer of data permitted to a country that does not have adequate data protection laws (no adequate privacy laws in the United States)
- **Directive 2002/58/EC** (July 12, 2002) concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector
  - Extension of opt-in beyond sensitive personal data
  - Right for mobile users to temporarily block the us of location data at any time
  - Cookies: only if user is informed, and user can reject them

LEGISLATIVE PROCESS IN EU

- Directive (e.g. Data Protection, Digital Signatures, Protection of Databases, Copyright) is first adopted by the EU Parliament
- Directive does not have the force of law per se in each Member State
- Each Member State must enact its own law implementing the provisions of the Directive
- Laws of each Member State, while consistent with the Directive, may differ from each other in materials ways
- Directive is the lowest common denominator

E.U. DATA PROTECTION OVERVIEW

Personal data must be:

- fairly and lawfully processed
- obtained only for specified and lawful purposes
- adequate, relevant and not excessive
- accurate and, where necessary, up to date
- processed in accordance with individual rights
- secure
- not transferred outside EEA (i.e. EU plus Norway, Iceland and Lichtenstein) without adequate security

PROTECTED INFORMATION

"Personal Data":

- Any information relating to an identified or identifiable natural person ("data subject")
- An identifiable person is one who can be identified, directly or indirectly, in particular by reference to
  - an identification number, or
  - one or more factors specific to the person's physical, physiological, mental, economic, cultural or social identify
- Information online or offline

SENSITIVE DATA

- Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, or concerning health or sex life is **prohibited**.
- Exceptions include:
  - Explicit consent, or
  - Employment
  - Processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent,e.g.
    - preventive medicine
    - medical diagnosis

ENTITIES SUBJECT TO COMPLIANCE

- “Data Controller”
  - Natural person, legal person, public authority or agency
  - Determines the purpose and means of the processing of the personal data
- “Data Processor”
  - Natural personal, legal person, public authority or agency
  - Processes personal data on behalf of the data controller

COVERED ACTIVITIES

- "Processing of Personal Data" includes
  - Any operation or set of operations that is performed on personal data, whether or not by automatic means, such as:
    - Collection
    - Recording
    - Organization
    - Storage
    - Adaptation or alteration
    - Retrieval
    - Disclosure by transmission
    - Consultation
    - Use
    - Dissemination
    - Alignment or combination
    - Blocking
    - Erasure
    - Destruction

SCOPE

- Processing of personal data wholly or partly by automatic means
- Processing other than by automatic means of personal data that form part of a filing system

- Not covered:
  - Activities of the States in areas of criminal law
  - Processing by natural person in the course of a purely personal or household activity

SCOPE (2)

- Processing is carried out in the context of the activities of a data controller established
  - on the territory of a member state; or
  - in a place where the national laws of a member state apply be virtue of international law; or
- Data controller is established outside the EU, and for purposes of data processing uses equipment situated in the EU (other than equipment used solely for the transit through the EU)

DATA QUALITY

All personal information must be:

- Processed fairly and lawfully
- Collected for specified, explicit and legitimate purposes
- Used only for the limited purpose first identified
- Adequate, relevant and not excessive in relation to the purposes for which the data are collected / processed
- Accurate, kept up to date
- Kept in a form, that permits identification of the data subjects for no longer than is necessary for the purposes for which the data were collected

LIMITATIONS TO DATA PROCESSING

Data may be processed only if:

- Data subject has unambiguously given his consent; or
- Processing is necessary for
  - performance of a contract to which the data subject is party
  - Compliance with controller's legal obligation
  - Protection of the data subject's vital interest
  - Performance of a task carried out in the public interest
  - Legitimate interests pursued by the controller of by the third party to whom disclosure is made

RIGHTS OF THE DATA SUBJECT

- Data subject must be informed:
  - That data is being collected
  - Identity of the data controller
  - Proposed uses of the information
  - Recipient or categories of recipients
  - Whether replies to questions are mandatory or voluntary, and the possible consequences of failure to reply
  - That he/she has the right to access to the data, and the right to rectify the data

RIGHT OF ACCESS AND AMENDMENT

Every data subject has the right to obtain

- Confirmation as to
  - whether or not data about him are being processes
  - the purpose of the processing
  - the categories of data concerned
  - the third parties to whom the data are disclosed
- Communication in an intelligible form of
  - the data undergoing processing, and
  - any available information as to their source
- Rectification, erasure or blocking of data that do not comply with the law (e.g. incomplete or inaccurate data)
- Notification of third parties to whom the data have been disclosed of any rectification, erasure, or blocking

CONSENT REQUIREMENTS

- Direct marketing:
  - Right to object, on request and free of charge, to the processing of data for marketing
  - Be informed, before personal data are disclosed for the first time to third parties, or used on their behalf for direct marketing, and to object, free of charge to disclosures
- Sensitive data:
  - Unambiguous consent required
  - “Sensitive data” = data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and data concerning health or sex life

CONFIDENTIALITY & SECURITY

- Data controller must implement technical and organizational security measures to protect against:
  - Accidental or unlawful destruction
  - Accidental loss
  - Alteration
  - Unauthorized disclosure or access
  - Unlawful forms of processing
- Data controller must enter into written contract with data processor
  - Processor will act only on instruction of data controller
  - Processor will implement security measures

REGISTRATION WITH SUPERVISORY AUTHORITY

- Data controller must “notify” (i.e. register with) the “Supervisory Authority” (i.e. the State Data Protection Agency) before performing any processing
- Information to be provided includes descriptions of:
  - Categories of data subjects
  - Categories of data to be collected
  - Recipients
  - Proposed transfers of data to third countries
  - Security measures
  - Information is kept in a register that may be inspected by anyone

TRANSBORDER DATA FLOW

- No transmission of data outside the EEA if the data are undergoing processing, or are intended for processing after the transfer unless the foreign country ensures an “adequate” level of protection (United States does not have such laws)
- Exception:
  - Unambiguous consent by the data subject (i.e. OPT-IN), or
  - Transfer is necessary for
    - Performance of a contract between the data subject and the controller
    - Performance or conclusion of a contract between controller and third party, which is for the benefit of the data subject
    - Protect vita interest of the data subject
    - Public interest
  - Data controller enters into a contract with the third party that ensures the same level of protection as provided under the EU state law
  - Commission finds that the third country ensures an adequate level of protection

COUNTRIES WITH ADEQUATE PROTECTION

- The EU Member States
- The EEA member countries:
  - Norway
  - Liechtenstein
  - Iceland
- The countries for which the Commission has determined that there is adequate data protection
  - Switzerland
  - Canada
  - Argentina
  - Isle of Man
  - Guernsey
  - NOT the United States
- Special: United States Department of Commerce Safe Harbor program

PROVIDING ASSURANCE TO EU PARTNER

- Before agreeing to transfer data to a US company, a company located in a EU/EEA member state will require that the US company provide assurances that the data will be “adequately protected”
- To provide this assurance, the US company can:
  - Take the benefit of the Safe Harbor program
  - Enter into a contract where it commits to provide the “adequate protection”

SAFE HARBOR

- US companies may join the Safe Harbor program administered by the DoC to assure of their adherence to 7 specific privacy principles.
- Self Certification procedure:
  - Description of the company's policies with respect to protection of personal data
  - Designate individual responsible for all questions regarding data protection
  - Must be renewed every year
- Enforcement:
  - by the FTC (but … beware of FTC Act Sect. 5, deceptive practices)
  - U.S. companies that qualify and register will be protected from prosecution or lawsuits by E.U. governments
- Information: www.export.gov/safeharbor

SAFE HARBOR PRINCIPLES

- To benefit from the Safe Harbor protection, a company must self certify that it complies with seven principles regarding the use and transfer of data:
  - 1. Notice
    - Inform data subjects of purpose for collection, third parties who may receive access
  - 2. Choice
    - Offer individuals opportunity to choose whether their personal information may be disclosed to third parties, or used for other purpose than the original purpose
  - 3. Transfer
    - Transfer data only to third parties with whom it has a written agreement, or who adhere to the Principles

SEVEN PRINCIPLES

- 4. Access
  - Individuals must have access to information about them, and be able to correct, amend or delete inaccurate information
- 5. Security
  - Take measures to protect from loss, misuse, unauthorized access, disclosure, alteration, destruction
- 6. Data Integrity
  - Not process information in a manner that it incompatible with the purpose for which it has been collected and authorized by the individual
- 7. Enforcement
  - Provide mechanisms for assuring and ensuring compliance with the Principles, recourse for individuals

SAFE HARBOR ISSUES

- Applies only to transfer from the EU, not the rest of the world
- Self-certification is limited to companies regulated by the FTC or Department of Transportation, e.g. excludes financial, credit card, telecom
- Subjects the company to FTC enforcement for Unfair Trade Practices (Section 5 of the FTC Act)
- Foreign subsidiary or distributor must nevertheless comply with its own local law

CONTRACTS

- EU Commission Standard Contractual Clauses
  - Standard clauses applying to controllers (June 15, 2001) (2001/497/EC)
  - Standard clauses applying to processors (December 27, 2001) (2001/16/EC)
  - http://europa.eu.int/comm/internal_market/privacy/modelcontracts_en.htm
- ICC Model Contracts
  - http://www.iccwbo.org/home/e_business/word_documents/Final%20version%20July%202002%20Model%20contract%20clauses.pdf

MODEL CONTRACT CLAUSES

- Only approved for transfer between the EU and US, uncertainty for transfers from other countries
- Data importer must process the data in accordance with mandatory principles (App.2)
- Data importer must agree to audit by the data exporter, or an inspector designated by the data exporter
- Transferor and transferee must agree that the data subject is entitled to compensation (third party beneficiary)
- Transferor and transferee are jointly and severally liable
- Governing law is that of the data exporter
- No variation permitted

PRIVACY IN CANADA

- Federal Laws
  - PIPEDA - Personal Information Protection and Electronic Documents Act
    - Implemented in 3 stages
      - 2001 Federally regulated organizations
      - 2002 Health information
      - 2004 All commercial activities
  - Privacy Act (1983) – federal government
- Provinces and Territories
  - Public sector:
    - Every province has privacy legislation governing the collection use and disclosure of personal information held by government agencies
  - Private Sector
    - Quebec

WHAT IS PII UNDER PIPEDA?

- Personal information includes any factual subjective information, recorded or not, about an identifiable individual. This includes information in any form, such as:
  - Age, name, ID numbers, income, ethnic origin, or blood type
  - Opinions, evaluations, comments, social status, or disciplinary actions
  - Employee files, credit records, loan records, medical records
- Does not include name, title, business address or telephone number of an employee of an organization.

PIPEDA's 10 PRIVACY PRINCIPLES

- Accountability
- Identify purposes
- Consent
- Limit collection to what is necessary
- Limit use, disclosure and retention
- Accuracy
- Safeguards
- Openness
- Individual access
- Ability for individuals to challenge compliance

PIPEDA v. EU PRIVACY

- Pipeda is gentle version of the EU data protection principles
- Sufficiently strong to be recognized by the EU Commission as offering “adequate data protection”
- But less strict. E.g., no requirement equivalent to the “Model Contract” requirements. Company, however, remains “accountable” , and can thus use its own data transfer agreements
- Business in Canada is not covered under the US Department of Commerce Safe Harbor self certifications.

QUESTIONS?

Françoise Gilbert

fgilbert@itlawgroup.com 650-804-1235 www.itlawgroup.com

Francoise Gilbert founded the *IT Law Group* after having practiced for over twenty years in large national or global law firms. The *IT Law Group* is based in Palo Alto, California and provides services and counseling to Fortune 500 and other global public companies through a network of affiliated technology law firms located in North America, Asia and the European Union.

Ms Gilbert focuses her practice on information technology transactions, information privacy and security matters, and international business. A recognized expert in information technology, and information privacy & security law, Ms. Gilbert has served as advisor to state governors, a senator and several trade associations. She has been an Adjunct Professor at the University of Illinois, Chicago Campus since the early 1990's. She serves on the Board of of Advisors of several silicon valley start-ups, and on the Board of Directors of the Bay Area Community Resources.

Ms. Gilbert holds Law Degrees from Paris University (France) and Loyola U of Chicago (USA), and undergraduate and graduate degrees in Mathematics. She is admitted to practice in California, Illinois and France.

Françoise Gilbert

fgilbert@itlawgroup.com

www.itlawgroup.com

650-804-1235